REMARKS

In the above-identified Office Action, the Examiner rejected Claims 1, 9 and 17 under 35 U.S.C. §102(e) as being anticipated by Banga et al. Claims 2 – 4, 10 – 12 and 18 – 20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Banga et al. in view of Chien et al. Claims 6 – 8 and 14 – 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Banga et al. in view of Chien et al. and further in view of Payton and Malagrino et al.

Examiner Fearer and Examiner Perez-Gutierrez are thanked for the interview of April 30, 2007. In that interview, Claim 1 and Banga et al., the primary reference, were discussed. Examiner Fearer and Examiner Perez-Gutierrez agreed that the reference did not teach the limitations in the last element of the claimed invention.

For the reasons stated more fully below, Applicants submit that the claims are allowable over the applied references. Hence, reconsideration, allowance and passage to issue are respectfully requested.

As disclosed in the Specification, data is generally transmitted on a network in packets. Before being transmitted, however, several headers may be added to the packets. One of the headers that may be added is an IP header. The IP header has a two-byte identification field that is used to facilitate packet fragmentations. For example, as a packet is traversing the network, routers may fragment the packet into smaller packets. To ascertain that a receiving host is able to reconstruct a packet after it has been fragmented in transit, a transmitting host will give the packet an identity by entering a number into the IP identification field. If a packet is fragmented, each fragment will retain the IP identification number in its IP header. When the receiving host receives the fragments, using the IP identification number along with other fields in the IP header, it will be able to reconstruct the packet.

The two-byte identification field allows for 65,536 unique IP packets to be generated before the IP identification numbers recycle. With the use of the

Gigabit Ethernet, however, this number of packets can be generated within one (1) second. Presently, it is rather common to have fragment re-assembly timers of thirty (30) seconds. Thus, using a fragment re-assembly timer of thirty (30) seconds with the Gigabit Ethernet may result in two or more packets having the same IP identification number on the network. When this occurs, if one or more fragments from a first packet are lost or dropped and if corresponding fragments from a second packet arrive at the receiving host within the 30-second re-assembly time of the first packet, the first packet may be re-assembled using the fragments from the second packet if the fragment offsets of the second packet match the fragment offsets of the first packet. Consequently, the re-assembled first packet will be erroneous. This error should in most cases be caught using a checksum value that is included in the IP header. Nonetheless, there may be times when the error may not be flagged by the checksum value. In these cases, erroneous data will be used.

Thus, what is needed is a method of ascertaining that fragments from two or more different packets that may have the same IP identification number are distinguishable from each other. The present invention provides such method.

According to the teachings of the invention, a method of reducing data corruption due to recycled Internet Protocol (IP) identification numbers is provided. The method comprises the steps of: determining whether packets are to be divided into fragments; determining, if packets are to be divided into fragments, whether IP identification numbers are being recycled; and setting a size of a first fragment of a packet to a maximum transmission unit (MTU), if the IP identification numbers are recycling and decrementing the size of the first fragment of a packet each time the IP identification numbers recycle.

The invention is set forth in claims of varying scopes of which Claim 1 is illustrative.

> 1. A method of reducing data corruption due to recycled Internet Protocol (IP) identification numbers comprising the steps of:

> determining whether packets are to be divided into fragments;
>
> ***determining, if packets are to be divided into fragments, whether IP identification numbers are being recycled***; and
>
> ***setting a size of a first fragment of a packet to a maximum transmission unit (MTU), if the IP identification numbers are recycling and decrementing the size of the first fragment of a packet each time the IP identification numbers recycle***. (Emphasis added.)

The Examiner rejected the independent claims as being anticipated by Banga et al. Applicants respectfully disagree.

Banga et al. purport to teach a prevention and detection of IP identification wraparound errors. According to the teachings of Banga et al., the prevention of IP identification wraparound errors is facilitated by using a plurality of number generators. Each number generator is associated with a receiving station or a plurality of number generators is associated with a plurality of receiving stations. When one number generator is associated with a receiving station, the IP identification number of a datagram that is to be transmitted to the receiving station is generated by the associated number generator. When a plurality of number generators is associated with a plurality of receiving stations, the plurality of number generators forms an array of number generators such as a 16-bit counter. Preferably, the plurality of number generators is associated with the plurality of receiving stations by hashing destination addresses for the receiving stations and protocols for transmitting to those receiving stations so as to form an index to the array.

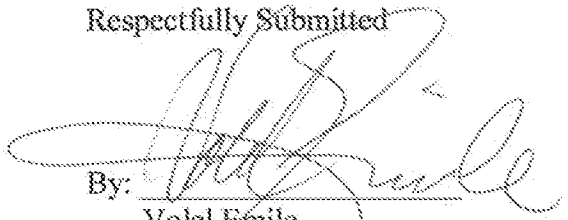
The detection of IP identification wraparound errors is facilitated by using a method of detecting a likelihood of mis-assembly of data fragments from fragmented IP datagrams. In this case, communication errors between a sending station and a receiving station are detected. The likelihood of mis-assembly is determined to be high upon detection that the communication errors occur at a high rate for a predefined period of time. The communication errors

that are detected can include communication errors detected by an IP layer of the receiving station's communication system. Such IP communication errors include, but are not limited to, receipt of overlapping data fragments and IP datagram reassembly timeout errors. The communication errors that are detected also can include communication errors detected by a UDP layer of the receiving station's communication system. Such UDP communication errors include, but are not limited to, UDP length errors and UDP checksum errors. The communication errors that are detected also can include communication errors detected by an NFS layer of the sending station's communication system.

However, Banga et al. do not teach, show or suggest the steps of ***determining, if packets are to be divided into fragments, whether IP identification numbers are being recycled***; and ***setting a size of a first fragment of a packet to a maximum transmission unit (MTU), if the IP identification numbers are recycling and decrementing the size of the first fragment of a packet each time the IP identification numbers recycle*** as in the claimed invention.

Since Banga et al. do not teach the emboldened-italicized limitations of the above-reproduced Claim 1, Applicants submit that Claim 1, as well as its dependent claims, is patentable over the applied references. The other independent Claims (i.e., Claims 9 and 17) as well as their dependent claims, which all incorporate the emboldened-italicized limitations of the above-reproduced Claim 1, are also patentable over the applied references. Hence, reconsideration, allowance and passage to issue are once more respectfully requested.

Respectfully Submitted



By: Volel Emile
Attorney for Applicants
Registration No. 39,969
(512) 306-7969